Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Elements of a Coexistence Protocol**
Date Submitted	**2005-04-27**
Source(s)	Rina Nathaniel Alvarion Tel Aviv, 21 HaBarzel Street Israel Voice: +972 3 7674287 Fax: +972 3 645 6204 mailto: Rina.Nathaniel@alvarion.com
Re:	Call for Contributions, IEEE 802.16h Task Group on License-Exempt Coexistence, IEEE 802.16h-05/007
Abstract	Propose messages and basics for a Coexistence Protocol and security considerations
Purpose	
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding o the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

Elements of a Coexistence Protocol

Rina Nathaniel

Alvarion

1. Introduction

The scope of the paper is to provide text for the IEEE 802.16h standard, to be inserted under section named "**Transmission of information**" see [1]. This proposal based on IEEE S802.16h – 05/006[2] and IEEE S802.16h – 05/008[3].

2. Background

Since the architecture for Radio Resource Management in the context of IEEE 802.16h is a distributed one and allows communication and exchange of parameters between different BSs, and in in session#35, a proposal of regional database for identifying the spectrum sharers has been accepted, we propose a protocol for communication between different Base Stations.

3. Messages

There are two types of messages, IP messages for communication between the BSs or with the Regional DB and 802.16 messages for BS ⇔ SS communication. The scope of this paper is restricted to BS⇔BS communication.

3.1 IP Messages

These messages are part of the Coexistence Protocol. Already some messages were proposed by ITRI. In addition, we propose messages addressing the interference management.

1. Get_Param
   - Messages between BSs, used to request the list of parameters
   - Parameters: list of the BS parameters

2. Evaluate_Interference
   - A message sent by a new BS wishing to use an existing Master sub-frame, to the BSs already acting as Masters, requesting them to evaluate its interference
   - Parameters: tbc.

3. Work_In_Parallel
   - A message sent by a new BS to request the use an existing Master sub-frame
   - Parameters: tbc.

4. Quit_sub_frame
   - A message sent by an old Base Station, in order to request the new Base Station to cease the operation as Master in the current sub-frame
   - Parameters: tbc.

5. Create_new_sub_frame
   - A message sent by a BSs to all the community BSs, to request the creation of a new Master sub-frame; the message will include: interfering BSIDs and the frame-number in which the change will take place
   - Parameters: tbc.

6. New_sub_frame_announce

- A acknowledgement to the previous message sent by the BSs in the community to the requesting BS, having as parameters: Frame-number for adding a sub-frame, New sub-frame number after the change, Master sub-frame number for the new Base Station
- Parameters: tbc.

7. Reduce_power
   - A message between a BS and an interfering BS requesting to reduce the power of the specified transmitter (identified by frame_number, sub-frame, time-shift) by P dB
   - Parameters: tbc.

8. Stop_operating
   - A message sent by a Master BS to the BSs operating in its Master sub-frame, but not being Masters for this sub-frame, requesting to cease using this sub-frame in parallel
   - Parameters: tbc.

3.2 Message Contents

3.2.1 Message Header

The message header contains the following fields:

- Version of protocol in use. This specification of the protocol is version 1.
- Message operation code (opCode);
- Flags indicating whether this message is a request or response
- Length of payload
- Message identifier (Message ID) for use in sequencing and retransmissions
- Association identifier (Association ID) for uniquely identifying an CP connection between a initiator and responder.

3.2.2 Message Payload

The following Type-Length-Value (TLV) tuples may be present in the CP payload depending on the message type:

Type	Parameter Description
tbc	**Operator ID**
tbc	**BS-ID**
tbc	**BS GPS coordinates**
tbc	**BS IP Address**
tbc	**MAC Frame duration**
tbc	**Type of sub-frame allocation**
tbc	**MAC Frame number chosen for the Master sub-frame**
tbc	**Sub-frame number chosen for the Master sub-frame**
tbc	**Repetition interval between two Master sub-frames, measured in MAC-frames**
tbc	**Time shift from the Master sub-frame start of the Base Station radio-signature transmission**
tbc	**Duration information for the Base Station radio-signature transmission**
tbc	**Repetition information for the Base Station radio-signature transmission**
tbc	**Time shift from the Master sub-frame start of the Subscriber Station radio-signature transmission**
tbc	**Duration information for the Subscriber Station radio-signature transmission**
tbc	**Repetition information for the Subscriber Station radio-signature transmission**
tbc	**List of other used sub-frames, in the interval between two Master sub-frames**
tbc	**Slot position**

3.3 Association

An Association ID is a parameter used to uniquely assign or relate a response to a request. The association identifier used on the responder and initiator MUST be a random number greater than zero to protect against blind attacks and delayed packets.

When the initiator sends subsequent messages, it uses the responder's association identifier in the Association ID field; when the responder sends a message it uses the initiator's association identifier in the Association ID field.

3.4 Sequencing and Retransmission

CP is a request-response protocol. In any particular message exchange, one party acts as the initiator (sends a request) and the other party acts as the responder (sends a response message).
The initiator sets the Message ID in the header to any value in the first message of the CP association, and increases the Message ID by one for each new request using serial number arithmetic. Retransmissions do not increment the Message ID. The responder sets the message ID in the response to the value of the message ID in the request.

The initiator is always responsible for retransmissions. The responder only retransmits a response on seeing a retransmitted request; it does not otherwise process the retransmitted *request.*
The retransmitted requests/responses are exact duplicates of previous requests/responses.

The initiator must not send a new request until it receives a response to the previous one. Packets with out-of-sequence Message IDs are considered invalid packets and are discarded.

The initiator must retransmit after a configurable interval until either it gets a valid response, or decides after a configurable number of attempts that the CP association has failed. (Since the retransmission algorithm is implementation-dependent, it is not defined here.)

3.5 Message Validity Check

A message is only accepted if all the following holds true:

- Message version field = 1.
- Association ID must match a current association
- All messages received by peer have R bit in flag set to zero
- All responses received by authenticator have R bit in flag set to one.
- Message opCode is valid
- Message length equals size of payload
- Message ID must match the expected sequence number
- The payload contains only those TLVs expected given the value of the opCode
- All TLVs within the payload are well-formed, TLVs marked as mandatory are recognized.

3.6 Fragmentation

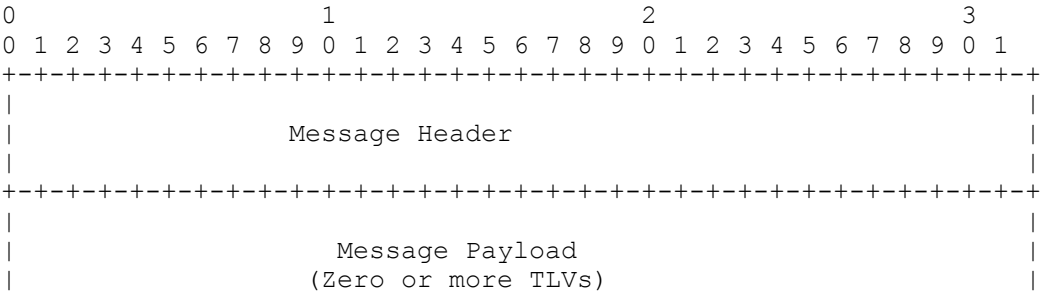
CP does not provide support for fragmentation.

3.7 Transport Protocol

CP uses UDP as the transport protocol with port number TBD. All messages are unicast.

3.8 Message Format

All messages are transmitted in network byte order. The message format has the following structure:



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The subsection below describes the format of the header and payload.

3.8.1 Header Format

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Flags        | Vers  |Opcode |              Length           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Message ID                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Association ID                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Flags - 8-bit field indicating options

```
      0 1 2 3 4 5 6 7
      +-+-+-+-+-+-+-+-+
      |M| Reserved    |
      +-+-+-+-+-+-+-+-+
```

Response Flag (R).
Set to 1 when message is a response to a request (same message ID). R must be zero in all request messages.
Reserved Flags: Reserved. Must be zero. MUST be cleared on sending and ignored on receipt

Version - 4-bit field indicating the version of this protocol. This specification = 1
OpCode - 4 bit field indicating CP message type
tbc
Length - Length of CP payload in octets excluding header
Message ID - Used to ensure ordered delivery and detect retransmissions.
Association ID - Uniquely identifies association in authenticator and peer.

3.8.2 Payload Format

The payload consists of zero or more type-length-value 3-tuples (TLVs).
Note: TLVs may not always start on a 4-byte boundary.

4 Security consideration

In this model, data traffic is protected by using IPsec.
The IP Security Protocol [IPsec] provides cryptographically based security for IPv4. The protection offered by IPsec is achieved by using one or both of the data protection protocols (AH and ESP). Data protection requirements are defined in the Security Policy Database (SPD). IPsec assumes use of version 2 of the Internet Key Exchange protocol [IKEv2], but a key and security association (SA) management system with comparable features can be used instead.

5. References

[1] IEEE 802.16h – 05/010 –Working Document for P802.16h, 2005-03-29
[2] IEEE C802.16h – 05/004r1 – General Architecture: Shared Radio Resource Management, 2005-04-26

[3] IEEE C802.16h – 05/008 - Proposal for 802.16h general operating principles, Mariana Goldhamer, Alvarion
[IPsec] http://www1.ietf.org/html.charters/ipsec-charter.html
[IKEv2] Internet Key Exchange (IKEv2) Protocol see http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-17.txt